Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2018/19
28. Nov. 2018

Übungen zur Vorlesung Kryptographie

Blatt 7

Aufgabe 25

Für eine zusammengesetzte ungerade Zahl $N = 2^t u + 1$, (u ungerade), sei

$$FW_{SS}(N) := \left\{ a \in (\mathbb{Z}/N)^* : a^{(N-1)/2} = \left(\frac{a}{N}\right) \right\}$$

die Menge der falschen Zeugen bzgl. des Solovay/Strassen-Tests und

$$FW_{MR}(N) := \left\{ a \in (\mathbb{Z}/N)^* : a^u = 1 \text{ oder } \exists k \in \{0, 1 \ldots, t-1\} \text{ mit } a^{2^k u} = -1 \right\}$$

die Menge der falschen Zeugen bzgl. des Miller/Rabin-Tests.

a) Man berechne die Anzahlen $\varphi(N)$, $\#FW_{SS}(N)$, $\#FW_{MR}(N)$ für die Carmichael-Zahlen

$$N = 561, 1105, 1729 \text{ und } 2000436751.$$

b) Man beweise: Für jede natürliche Zahl $N \equiv 3 \bmod 4$ gilt

$$FW_{SS}(N) = FW_{MR}(N).$$

Aufgabe 26 (Fortsetzung von Aufgabe 25)

Seien q, p ungerade Primzahlen mit $p = 2q - 1$.

[Beispiele dafür sind $(q, p) = (3, 5)$, $(7, 13)$, $(19, 37)$, $(31, 61)$, $(37, 73), \ldots$].

Man zeige: Für $N := pq$ gilt

$$\#FW_{SS}(N) = \frac{\varphi(N)}{4}.$$

Aufgabe 27

Der Fermatsche Algorithmus zur Faktorisierung einer zusammengesetzten ungeraden Zahl $N \geqslant 9$ arbeitet wie folgt: Mit $x_0 := \lceil \sqrt{N} \rceil$ berechne man für $x := x_0 + k$, $k = 0, 1, 2, 3, \ldots$, der Reihe nach die Differenzen $x^2 - N$, bis sich eine Quadratzahl ergibt:

$$x^2 - N = y^2.$$

Dann ist $N = (x - y)(x + y)$ eine nicht-triviale Faktorzerlegung von N.

---

b.w.

a) Man zerlege folgende Zahlen mit dem Fermatschen Algorithmus:

$$N_1 := 551, \quad N_2 := 1643, \quad N_3 := 2479.$$

b) Man beweise, dass der Algorithmus stets nach einer endlichen (möglicherweise großen) Anzahl von Schritten erfolgreich ist.

c) Sei $N = uv$ mit positiven ganzen Zahlen u, v, die der Abschätzung $|u - v| \leqslant \alpha\sqrt[4]{N}$ mit einer reellen Konstanten α genügen. Man schätze (als Funktion von α) die Anzahl der Schritte ab, die der Fermatsche Algorithmus zur Faktorisierung von N braucht.

Aufgabe 28

Um ein RSA-System mit Modul $N = pq$, wobei $2^{2m-1} < N < 2^{2m}$, (z.B. $m = 512$) aufzustellen, wird empfohlen, die Primzahlen p, q so zu wählen, dass

$$|p - q| \geqslant 2^{m-7}.$$

a) Warum ist das Fermatsche Faktorisierungs-Verfahren zur Faktorisierung von N dann ungeeignet?

b) Im folgenden Beispiel eines RSA-Moduls N wurde diese Empfehlung nicht beachtet. In hexadezimaler Schreibweise ist

```
 N = 8FCB CBFF F085 731F 2B06 E71B 8AD5 C5D2 7E87 B7F0 A91D 0AEA B4FF 7020
99DC DC28 19D2 BE76 028C D0D7 7F77 CD8E BEFC 567A 195E 2F03 E94F E04C 1D23
26C9 6F64 6265 35E5 9996 F0B2 CA7F C9A7 F316 3A53 FE49 7F90 71CF 9DF8 64A7
6EC8 99D8 5661 A7AB E5E9 A603 F1BC 4196 17EB 1341 A0BD 4300 B36F C2B7 43E1
A7DF FD4A CF80 BBEB 1463
```

Der Verschlüsselungs-Exponent ist $e = 2^{16} + 1$. Man enschlüssele den folgenden Geheimtext

```
0B79 F5BB D903 4FCE B8AF 5097 49EB 7B79 63B7 EC15 E220 2F09 3F53 9493 2623
C5FC 4F02 C8D4 AEB5 CCBA 1EBF A4AA 06CF 71E0 D61F 0A72 E7AD BC1B 585D E909
7CCE C340 EF0A 1B90 0976 9FDD 7E1B C4C0 B103 F219 0DDB CA3C 4B41 29F4 F19E
4C51 8F82 38A4 8414 7EF7 B99B 0611 0A3C 92A1 FC19 555C 16BE 773B A58A EE8C
258F CDF8 D709 8339
```

Dieser entstand aus einem Ascii-Klartext $(a_1, a_2, \ldots, a_n)$, $0 \leqslant a_i < 256$, der durch die ganze Zahl

$$x = \sum_{i=1}^{n} a_i \cdot 2^{8(n-i)}$$

dargestellt wurde.